HARRY SHULMAN (SBN 209908)
SHULMAN LAW
44 MONTGOMERY STREET
SUITE 3830
SAN FRANCISCO, CA 94104
415-901-0505
415-901-0506 (fax)
harry@shulmanlawfirm.com

Attorney for Plaintiffs
Additional attorneys on signature page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

Nick Ialacci, Cade Miller, Samuel Smith, Terry Shapiro, Dawn Johnson, Zachary Goodale, Jay Loeffel, and Bradley Miller, individually and on behalf of all others similarly situated, Plaintiffs, v. Equifax, Inc., Defendant.	**CIVIL ACTION NO:** **COMPLAINT FOR NEGLIGENCE; AND VIOLATIONS OF FCRA, STATE CONSUMER PROTECTION STATUTES, AND STATE DATA BREACH STATUTES** **DEMAND FOR JURY TRIAL** **CLASS ACTION**

By and through their undersigned counsel, Plaintiffs, individually and on behalf of all others similarly situated, bring this action for damages and injunctive relief against Defendant Equifax, Inc. ("Equifax"). Plaintiffs allege, based on information and investigation of counsel, as follows:

NATURE OF THE ACTION

1. On September 7, 2017, Equifax announced one of the largest and most severe data breaches in history (referred to hereinafter as the "Equifax Data Breach"), admitting

that the personal and confidential information of as many as 143 million Americans – almost half the country's population – had been compromised or disclosed to unauthorized third parties between mid-May and July 2017.[1]

2. The information accessed included names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers (this information is commonly referred to as personally identifiable information ("PII")). In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with PII for approximately 182,000 U.S. consumers, were accessed.[2]

3. This is a consumer class action suit brought by Plaintiffs, individually and on behalf all other similarly situated persons whose PII and credit account information was made accessible to thieves or other third parties after being entrusted to, and while in the possession, custody, and control of, Defendant Equifax. This information is private and sensitive in nature, and Equifax failed to adequately protect it. Equifax did not obtain consent or permission from Plaintiffs or any of the Class members to disclose their PII, credit account, or other personal and confidential information to any other person or entity, as would be required for such disclosure by applicable law and industry standards prior to any such disclosure.

4. Equifax discovered the data breach in July 2017, but failed to publicly report it or otherwise alert those affected until September 7, 2017, when it finally issued a press release.[3]

---

[1] CNN, http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/ (last visited Sept. 19, 2017).

[2] Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), *available at* https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[3] When Equifax did get around to letting anyone know the breach had occurred, it directed those affected to a website where Equifax asked them to disclose even more PII and tried to sell them the company's own credit monitoring service. *See* Fortune Insider,

5. In its press release, Defendant Equifax failed (or refused) to provide any substantive information as to how the breach actually occurred, choosing instead to attribute it to an unspecified "application vulnerability."[4] Apparently trying to downplay its significance, Equifax Chairman and Chief Executive Officer Richard Smith dismissively described the Equifax Data Breach as "a disappointing event for our company."[5]

6. The Equifax Data Breach is even more "disappointing" for those, including Plaintiffs and the Class members, who are among the 143 million Americans who have had their most sensitive PII and credit account information exposed by reason of Equifax's conduct in: (a) failing to adequately protect that information; (b) failing to inform Plaintiffs and the Class members that it did not have adequate systems or security processes, protocols, or practices in place to safeguard that information; (c) failing to prevent the Equifax Data Breach from occurring; (d) failing to mitigate the effects of the Equifax Data Bread; and (e) failing to provide timely notice of the Equifax Data Breach after its occurrence.

7. Ultimately, Equifax intentionally, willfully, recklessly and/or negligently failed to protect the PII and credit account information of Plaintiffs and the Class members from unauthorized disclosure. As a result, Plaintiffs and the Class members have been damaged and remain at substantial and continuing likelihood for identity theft/fraud. Indeed, financial experts have opined that victims of a data breach are 9.5 times more likely to be a victim of identity fraud that are members of the general public.[6] Accordingly,

---

Is Equifax Going to Be Punished for Losing Our Data? (Sept. 12, 2017), *available at* http://fortune.com/2017/09/12/equifax-data-breach-2017-security-hacked/.

[4] *Id.*

[5] *Id.*

[6] Intersections, Inc., *Identity Fraud Rose in 2011 Based on Findings from the Recently Release 2012 Identity Fraud Report by Javelin Strategy & Research* (Feb. 22, 2012), *available at* http://invest-media.intersections.com/phoenix.zhtml?c=175233&p=irol-newsArticle_Print&ID=1663910.

Plaintiffs and the Class members now "need to be hyper vigilant and monitor their accounts" for fraudulent activity.[7]

8. As a direct and proximate result of Equifax's intentional, willful, reckless and/or negligent acts and omissions, of its violation of state and federal statutes, and of the resulting Equifax Data Breach, over 143 million individuals in the United States – including Plaintiffs and the Class members – have had their PII and credit account information exposed to fraud and identity theft, and have suffered injuries including but not limited to:

a. theft or misuse of their personal and financial information;

b. substantial immediate and continuing likelihood for identity theft/fraud;

c. costs associated with the detection and prevention of identity theft/fraud and unauthorized use of their personal information and/or financial accounts;

d. unauthorized charges on their debit and credit accounts;

e. lost use of, or limitation of access to, account funds and costs associated therewith, including missed payments on bills or loans, late charges and fees, negative effects on credit (e.g., decreased credit scores and adverse credit notations), etc.;

f. loss of productivity and other costs associated with efforts necessary to ameliorate or mitigate the present and future consequences of the Equifax Data Breach, including watching for and finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax Data Breach;

[7] CBS News, *Equifax hack "basically the Irma of data breaches," expert says* (Sept. 8, 2017), *available at* https://www.cbsnews.com/news/equifax-hack-basically-the-irma-of-data-breaches-expert-says/.

g. damages to, and diminution in value of, their personal and financial information, which was entrusted to Equifax for the sole purpose of reporting and/or monitoring their credit profiles and with the mutual understanding that Equifax would safeguard that information from access, theft, or misuse;

h. money paid for products or services purchased from Equifax (e.g., credit monitoring, credit score inquiry) prior to the Equifax Data Breach, as Plaintiffs and the Class members would not have purchased such products or services had Equifax disclosed its lack of adequate security systems, processes, and protocols to reasonably safeguard their personal and financial information; and/or

i. continued substantial risk to their personal and financial information, which remains in the possession of Equifax and which is subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect it.

9. Plaintiffs, on behalf of themselves and all others similarly situated, seek to remedy these harms, and to prevent their future occurrence. To that end, they are asserting claims against Equifax for negligence, violations of the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681, *et seq.*; violation of state consumer protection laws, and violation of state data breach statutes. They seek to recover damages, including actual and statutory damages, to obtain equitable relief (including injunctive relief, restitution, disgorgement), and to recover costs and reasonable attorney fees as permitted by law.

10. Plaintiffs have standing to bring this class action on behalf of themselves and the Class members because they were damaged as a direct and proximate result of Equifax's wrongful conduct and the Equifax Data Breach resulting therefrom.

PARTIES

A. PLAINTIFFS

11. Plaintiff Nick Ialacci is a resident of Los Angeles County, California. As confirmed by Equifax, Plaintiff Ialacci's PII and/or credit account information was

included in the Equifax Data Breach and was disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

12. Plaintiff Samuel Smith is a resident of Denver Colorado. As confirmed by Equifax, Plaintiff Smith's PII and/or credit account information was included in the Equifax Data Breach and was disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

13. Plaintiff Terry Shapiro is a resident of Lakeworth, Florida. As confirmed by Equifax, Plaintiff Shapiro's PII and/or credit account information was included in the Equifax Data Breach and was disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

14. Plaintiff Dawn Johnson is a resident of Glencoe, Illinois. As confirmed by Equifax, Plaintiff Johnson's PII and/or credit account information was included in the Equifax Data Breach and was disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

15. Plaintiff Cade Miller is a resident of Edina, Minnesota. As confirmed by Equifax, Plaintiff Cade Miller's PII and/or credit account information was included in the Equifax Data Breach and was disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

16. Plaintiff Zachary Goodale is a resident of Dover, New Hampshire. As confirmed by Equifax, Plaintiff Zachary Goodale's PII and/or credit account information was included in the Equifax Data Breach and was disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

17. Plaintiff Jay Loeffel is a resident of New York, New York. As confirmed by Equifax, Plaintiff Loeffel's PII and/or credit account information was included in the Equifax Data Breach and was disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

18. Plaintiff Bradley Miller is a resident of Appleton, Wisconsin. As confirmed by Equifax, Plaintiff Bradley Miller's PII and/or credit account information was included in the Equifax Data Breach and was disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

19. As a direct and proximate result of Defendant Equifax's wrongful acts or omissions (as set forth fully herein) and the resulting data breach, each Plaintiff, and each of the Class members, has suffered actual harm and has been placed at imminent substantial and continuing risk for identity theft or identity fraud (as Equifax has conceded in its recent press releases and by its creation of a urging consumers to sign up for credit file monitoring and identity theft protection).[8]

20. As a direct and proximate result of Defendant Equifax's wrongful acts or omissions and the resulting Equifax Data Breach, each Plaintiff, and each Class member, has spent time, and will continue to spend time and effort in the future, monitoring their financial accounts. Additionally, the PII and/or credit account information of each Plaintiff and each Class member has been placed at a substantially increased risk of identity fraud/theft or other misuse, thus requiring them to take protective measures they would not have had to take but for the Equifax Data Breach. Any additional misuse of Plaintiffs' or the Class members' PII or credit account information will result in additional damages.

B. DEFENDANT

21. Defendant Equifax is a Georgia corporation with its headquarters in Atlanta, Georgia.

22. Defendant Equifax has numerous offices throughout California and in this District, including in Palo Alto, San Rafael, Concord, Panorama City, and Moonpark.

[8] *See* Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), *available at* https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

Further, TrustedID, Equifax's wholly-owned subsidiary and provider of credit monitoring services following the Equifax Data Breach, is headquartered in Palo Alto, California.

23. Defendant Equifax is a "consumer reporting agency" within the meaning of the FCRA – specifically 15 U.S.C. § 1681a(f) – in that Equifax, "for monetary fees . . . regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."

JURISDICTION

24. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because Plaintiffs' FCRA claims arise under the laws of the United States.

25. This Court has also has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because at least one class member is a citizen of a state that is diverse from Defendant Equifax and the amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 Class members.

26. This Court has personal jurisdiction over Defendant Equifax because: (a) it regularly transacts business in the California (and the other 49 states) and in this District; (b) it intentionally avails itself of this jurisdiction by directly or indirectly marketing and selling its goods or services throughout the United States, including in this District; (c) it has substantial aggregate contacts with this District; and/or (d) it has purposefully availed itself of the laws of the United States and the State of California.

VENUE AND INTRADISTRICT ASSIGNMENT

27. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this

District, including the actions of Trusted ID, which is a wholly owned subsidiary of Defendant Equifax located in Santa Clara county.

28. For the same reason, this case should be assigned to the Court's San Jose division.

FACTUAL ALLEGATIONS

29. The FCRA was enacted to promote the accuracy and privacy of consumer information contained in the files of consumer reporting agencies, and it regulates the collection, dissemination, and use of consumer information, including consumer credit information.

30. Consumer reporting agencies ("CRAs") are entities that collect and disseminate information about consumers to be used for credit evaluation and certain other statutorily enumerated purposes, including employment. There are three major CRAs, of which Defendant Equifax is one (the other two being TransUnion and Experian).

31. As a CRA, Equifax knows or should know of its legal obligations regarding the protection of sensitive consumer personal and credit information, as those obligations are clearly defined in the FCRA, federal regulations enacted pursuant thereto,[9] and promulgations of the Federal Trade Commission (FTC).[10]

32. In 1899, Equifax was founded in Atlanta, Georgia as a Retail Credit Company. It currently organizes, assimilates, and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers.

[9] *See, e.g.*, 15 C.F.R. Part 600, Appendix A to Part 601 - - Prescribed Summary of Consumer Rights; Appendix B to Part 601 - - Prescribed Notice of Furnisher Responsibilities; Appendix C to Part 601 - - Prescribed Notice of User Responsibilities.

[10] *See, e.g.*, 55 Fed. Reg. 18805 (May 4, 1990), Statement of General Policy or Interpretation; Commentary on the Fair Credit Reporting Act;

33. Ironically, Equifax touts itself as a leader in cybersecurity, and assures those who use its services that they can "FEEL CONFIDENT" knowing they are protected by "daily credit monitoring," which will purportedly detect "fraud, unexpected charges, [and] unauthorized credit inquiries."[11]

34. The personal and financial information that Equifax collects on consumers, including their names, Social Security numbers, credit account information, etc., is extremely valuable. Indeed, there exists on the internet a "cyber black-market" on which criminals openly post stolen credit/debit card numbers, Social Security numbers, and other personal information.

35. The FTC has advised consumers to guard this information carefully,[12] noting that it is "what thieves use most often to commit fraud or identity theft,"[13] and warning that once they have it, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[14] In short, "[f]or identity thieves, this information is good as gold,"[15] and they have used it to steal approximately $112 billion over the past 6 years.[16]

36. Given the foregoing, it is not surprising that the PII and credit account information Defendant Equifax exposed in the subject breach is highly coveted and aggressively sought by hackers, who use that information for any number of fraudulent purposes over the course of time; e.g., committing identity theft/fraud, perpetuating

---

[11] https://web.archive.org/web/20161025172308/http://www.equifax.com/home/en_us (last visited Sept. 19, 2017).

[12] FTC, *Protecting Personal Information: A Guide for Business*, (Oct. 2016) *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[13] *Id*.

[14] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

[15] https://www.identitysafetyservices.com/how-your-identity-is-stolen.php

[16] https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point

immigration fraud, obtaining false driver's licenses, using the victims' information to obtain government benefits, filing tax returns in the victims' name to obtain fraudulent refunds, etc.[17]

37. According to a study conducted by the U.S. Government Accountability Office, "stolen data may be held for a year or more before being used to commit identity theft," and "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[18] In other words, "[i]f any of the data was exposed, you will be living with that for the rest of your life."[19]

38. Thus, Plaintiffs and the Class members are confronted with a substantial and continuing risk that they will be the victims of identity theft (if they have not been already), and they will have to carefully and constantly monitor their personal and financial information, incurring damages associated therewith.

39. Once a victim becomes aware he has been the victim of identity theft and has suffered financial losses as a result thereof, simply reimbursing those losses does not make the victim whole as he must devote significant time (and money) to repairing the damage that has been done. In this regard, the Department of Justice's Bureau of Justice Statistics confirms that victims of identity theft "reported spending an average of about 7 hours clearing up the issues" caused by the theft, with many individuals having to spend much longer.[20]

40. In addition to being of critical importance to Plaintiffs and the Class members, the sensitive financial and personal data exposed in the Equifax Data Breach is

[17] Class Action Reporter, *Chipotle Data Breach Class Action*, *available at* http://www.classactionsreporter.com/consumer/chipotle-data-breach-class-action.
[18] *See* GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf
[19] WRAL.com, *What you need to know about the Equifax data breach* (Sept. 9, 2017), http://www.wral.com/what-you-need-to-know-about-the-equifax-data-breach/16937270/.
[20] Erika Harrell, *Victims of Identity Theft, 2014*, U.S. DEPT. OF JUSTICE (Sept. 2015), *available at* https://www.bjs.gov/content/pub/pdf/vit14.pdf.

the lifeblood of Equifax itself, which currently employs roughly 9,900 people worldwide, and which operates, or has investments, in two dozen countries spread across North, Central and South America, as well as Europe and Asia.

41. Equifax operates in four segments: U.S. Information Solutions, International, Workforce Solutions, and Global Consumer Solutions. Its products and services are based on databases of consumer and business information derived from various sources, including credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data. Even the Social Security Administration uses Equifax to help verify the identity of individuals who set up Social Security accounts on www.ssa.gov.

42. Equifax has enjoyed wide growth and massive financial success based on its use of sensitive financial and personal consumer data. From 2015 to 2016, Equifax experienced an 18% growth in operating revenues (to $3.14 billion). It currently has a market capitalization of over $14 billion, and last year its CEO was rewarded with a total compensation package of nearly $15 million.

43. Given the foregoing, it is evident that Equifax has (and had) the necessary resources to obtain and implement appropriate security measures to ensure the Equifax Data Breach did not occur. Unfortunately, it neglected, refused, or otherwise failed to do so.

A. The Equifax Data Breach.

44. On September 7, 2017, Equifax issued a press release announcing that "[c]riminals exploited a U.S. website application vulnerability to gain access to certain files" in Equifax's systems.[21] Although the press release was not issued until September, Equifax knew about the breach as early as July 29, 2017.

[21] [21] Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), *available at* https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

45. In its September 2017 press release, Equifax acknowledged that the information disclosed consisted "primarily" of PII, including names, Social Security numbers, birth dates, and addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed."[22]

46. The breadth of the Equifax Data Breach is stunning, as Defendant itself concedes, having admitted that it impacted "approximately 143 million U.S. consumers."[23] Per Seena Gressin, an attorney in the FTC's Division of Consumer & Business Education, "[i]f you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies."[24]

47. Ultimately, experts suggest that as much as 44% of the U.S. population will be affected, especially with regard to social security numbers, which rarely change over a person's lifetime, and which therefore hold substantial resale value on the black market.[25]

B. Equifax knew it was vulnerable to a data breach, but failed to take adequate precautions to prevent its occurrence or mitigate its severity.

48. Equifax knew or should have known it was vulnerable to attack based on the occurrence of previous data breaches and prior reports that its internal protections were

[22] *Id.*
[23] *Id.*
[24] FTC, *The Equifax Data Breach: What to Do* (Sept. 8, 2017), *available at* https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.
[25] Lily Hay Newman, *How to Protect Yourself From that Massive Equifax Breach*, WIRED (Sept. 7, 2017), *available at* https://www.wired.com/story/how-to-protect-yourself-from-that-massive-equifax-breach/.

outdated and weak. Indeed, Equifax has "had problems protecting its customers' information dating back years."[26]

49. In 2016, for example, Equifax's W-2 Express website was the subject of a cyberattack that resulted in the leak of over 400,000 names, addresses, social security numbers, and other personal information of employees who worked for the retail firm Kroger. The breach resulted in a lawsuit, which was ultimately dismissed without prejudice after Equifax agreed to fix the "glaring security issue" that caused the breach (though it is unclear whether Equifax ever actually did fix the problem).[27]

50. Also in 2016, Equifax suffered another data breach involving TALX, one of its subsidiaries that provides online payroll, HR, and tax services.[28] This breach was especially alarming because Equifax failed to discover it for almost a year (from April 17, 2016 through March 29, 2017), and because once it did discover the breach, Equifax waited over a month to disclose it.[29]

51. Equifax also suffered data breaches in January 2017, when the credit information of a "small number" of LifeLock customers was exposed, and in 2013-2014, when Equifax admitted to the New Hampshire attorney general that an "IP address operator was able to obtain the credit reports using sufficient personal information to meet Equifax's identity verification process."[30]

---

[26] *A Brief History of Equifax Security Fails*, Forbes.com (Sept. 8, 2017) (available at https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#3d4a854a677c)

[27] *Id.*

[28] Krebs On Security, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division* (May 18, 2017), *available at* https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/.

[29] *Id.*

[30] *A Brief History of Equifax Security Fails*, Forbes.com (Sept. 8, 2017) (available at https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#3d4a854a677c)

52. In 2016, security experts discovered "a common vulnerability known as cross-site scripting (XSS) on the main Equifax website." XSS is a process by which an attacker can create a link, which they then send to Equifax customers. If the target clicks the link and logs into the site, his username and password can be revealed to the attacker, thereby exposing the target's personal information.[31]

53. Other security experts (namely Kenneth White and Kevin Beaumont) have probed Equifax's infrastructure and learned it was susceptible to attacks because it uses old or discontinued technology. For example, White discovered a link in the source code on the Equifax consumer sign-in page pointing to Netscape, a web browser that was discontinued in 2008. Per Beaumont, "Equifax's infrastructure is a weird mix of IBM WebSphere, Apache Struts, Java . . . it's like stepping back in time a decade."[32]

54. Jeff Williams, co-founder and Chief Technical Officer of Contract Security, concurs, having explained that two flaws in the above-referenced Apache Struts software "jump out as possibilities" for causing the Equifax data breach; specifically, CVE-2017-5638, an expression language vulnerability, and CVE-2017-9085, an HTTP request with an unsafe serialized object.[33]

55. Per Apache Struts Vice President Rene Gielen, Equifax was notified of the CVE-2017-5638 vulnerability in March 2017, and was provided with "clear and simple instructions of how to remedy the situation."[34] In the time between (a) learning of vulnerability and the patch that would have fixed it, and (b) the commencement of the

---

[31] *Id.*

[32] *Id.*

[33] Teri Robinson, *Apache Struts vulnerability likely behind Equifax breach, Congress launches probes* (Sept. 12, 2017), *available at* https://www.scmagazine.com/apache-struts-vulnerability-likely-behind-equifax-breach-congress-launches-probes/article/687955/.

[34] Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017), *available at* https://www.wired.com/story/equifax-breach-no-excuse/.

Equifax Data Breach, Equifax did nothing, thus ensuring it was "relatively easy" for the attackers to gain access to its servers and network.[35]

C. Equifax concealed the data breach while its executives sold their stock.

56. As noted previously, Equifax learned of the unauthorized access on July 29, 2017. Rather than immediately notifying those affected, Equifax concealed the existence of the breach for over a month. Its conduct in doing so is in direct contravention of its own recognition that a quick response is of critical importance when personal and financial information has been exposed. Indeed, Equifax states on its website that "[k]nowledge is the best line of defense when it comes to identity theft. The more you know, the better position you'll be in if you're ever a victim."[36] Equifax goes on to instruct that anyone whose personal information has been compromised should "[s]tart monitoring all your accounts."[37] It also admits that: (a) "the sooner you find out about the problem, the less time has lapsed in which the thief can use your identity;" and (b) "[t]he longer the individual's personal information is used unnoticed, the more damage is done and the longer it may take to clean up."[38] Equifax concludes by advising consumers to "act quickly, take good notes, and stay organized. Make sure to take care of yourself emotionally, as identity theft has many [effects] on victims more far-reaching than the most widely known financial impact."[39]

57. Instead of acting quickly to alert the public of its latest massive data breach, top Equifax executives – namely Chief Financial Officer John Gamble, Jr., Workforce Solutions President Rodolfo Ploder, and U.S. Information Solutions President Joseph Loughran – executed over $1.8 million in stock options approximately two days after

---

[35] *Id.*
[36] Equifax, https://www.equifax.com/personal/ (Learn about Identity Theft tab).
[37] https://blog.equifax.com/identity/my-identity-has-been-stolen-now-what/
[38] *Id.*
[39] *Id.*

Equifax learned of the breach, but long before it publicly reported its occurrence.[40] None of the accompanying regulatory filings lists the transactions as being part of 10b5-1 scheduled trading plans.

D. The post-breach monitoring Equifax has offered is inadequate and deceiving.

58. After the subject data breach occurred, Equifax told its customers it had "established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted" by the breach and to enable them "to sign up for credit file monitoring and identity theft protection."[41]

59. The Equifax breach website says that, in addition to people impacted by the data breach, Equifax is also offering one year of free TrustedID Premier services to anyone in the United States, "[r]egardless of whether your information may have been impacted."[42]

60. By encouraging all consumers to sign up for TrustedID Premier, Equifax stands to profit significantly from the breach it allowed to happen, and it exposes consumers to additional risks.

61. In order to register for Equifax's post-breach monitoring, consumers are required to provide six digits of their social security number, which is problematic because an individual's entire Social Security Number can be ascertained with just those six digits. To determine an individual's entire Social Security number an attacker would only have to figure out the first three digits, which is not a difficult task.

---

[40] Todd Haselton & Yen Nee Lee, *Three Equifax executives sold $2 million worth of shares days after cyberattack*, CNBC (Sept. 7, 2017), *available at* https://www.cnbc.com/2017/09/07/equifax-cyberattack-three-executives-sold-shares-worth-nearly-2-million-days-after-data-breach.html.

[41] Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), *available at* https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[42] *Id*.

62. Social Security numbers consist of nine digits made up of three parts; the first set of three digits is the Area Number, the second set of two digits is the Group Number, and the final set of four digits is the Serial Number.

63. Part one, the Area Number, indicates the geographical region in which the person applied for a social security card. Prior to 1972, states had field offices that issued social security cards and the Area Number assigned represented the state in which the card was issued. In 1972, however, the Social Security Administration began issuing cards from a central location and stopped using the state-based Area Numbers. Since 1972, the Area Number is based on the zip code in the mailing address provided on the original application for the Social Security card. Through a little digging or a credit report listing all residences obtained from the Equifax data breach, an immoral actor could easily piece together the full Social Security number.

E. Over 140 million Americans, including Plaintiffs and the other Class members, suffered injuries as a direct and proximate result of the Equifax data breach.

64. Because of the nature of the information exposed by the Equifax Data Breach (i.e., Social Security numbers, birth dates, driver's license numbers, consumer credit information), Plaintiffs and the Class members face an imminent, continuing, and substantial risk of identity theft. In addition to fears commonly associated with such identity theft (e.g., fraudulent credit card use, the opening of unauthorized accounts, harm to a credit score) there are additional consequences, including medical identity theft (fake IDs used to pay for procedures and surgeries), tax fraud (filing false tax returns to profit from refunds), and synthetic identity theft (combining information from multiple victims to create a new identity).

65. As a direct and proximate result of the Equifax data breach, Plaintiffs and the other Class members have suffered injuries, including but not limited to: (a) theft or misuse

of their personal and financial information; (b) substantial immediate and continuing likelihood for identity theft/fraud; (c) costs associated with the detection and prevention of identity theft/fraud and unauthorized use of their personal information and/or financial accounts; (d) unauthorized charges on their debit and credit accounts; (e) lost use of, or limitation of access to, account funds and costs associated therewith, including missed payments on bills or loans, late charges and fees, negative effects on credit (e.g., decreased credit scores and adverse credit notations), etc.; (f) loss of productivity and other costs associated with efforts necessary to ameliorate or mitigate the present and future consequences of the Equifax Data Breach, including watching for and finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax Data Breach; (g) damages to, and diminution in value of, their personal and financial information, which was entrusted to Equifax for the sole purpose of reporting and/or monitoring their credit profiles and with the mutual understanding that Equifax would safeguard that information from access, theft, or misuse; (h) money paid for products or services purchased from Equifax (e.g., credit monitoring, credit score inquiry) prior to the Equifax Data Breach, as Plaintiffs and the Class members would not have purchased such products or services had Equifax disclosed its lack of adequate security systems, processes, and protocols to reasonably safeguard their personal and financial information; and (i) continued substantial risk to their personal and financial information, which remains in the possession of Equifax and which is subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect it.

CLASS ALLEGATIONS

66. Plaintiffs bring this action both on behalf of themselves and all others similarly situated (the "Class") pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2) and (b)(3). The Class is defined as follows:

> All residents of California, Colorado, Florida, Illinois, Minnesota, New Hampshire, New York, and Wisconsin whose PII and/or credit account information was stolen or exposed in the Equifax Data Breach from May of 2017 through the present.

67. Following further investigation as and discovery in the case, the Class definition, including the Class Period, may be modified by amendment, and Plaintiffs reserve the right to join additional class representatives.

68. *Numerosity.* The Class is so numerous that joinder of all members is impracticable. Even though the exact number of Class members is unknown at this time, Equifax has represented that at least 143 million individuals have been affected by the Equifax Data Breach, and it has admitted that their identities can be readily ascertained from records already in its possession.

69. *Ascertainability.* All members of the purposed Classes are readily ascertainable. Equifax has access to addresses and other contact information for millions of Class members, which can be used for providing notice to many Class members.

70. *Typicality.* Plaintiffs' claims are typical of the claims of the other members of the Class because the events and conduct that give rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member. Plaintiffs and the Class members were similarly affected by the Equifax's uniform wrongful and unauthorized disclosure of personal, confidential information to unauthorized third parties.

71. *Adequacy.* Plaintiffs will fairly and adequately protect the interests of the Class and have retained counsel competent and experienced in class action and consumer

protection litigation. Plaintiffs' interests are coincident with, and not antagonistic to, the interests of the Classes.

72. *Commonality.* Common questions of law and fact exist as to all members of the Class, and these common questions predominate over any questions solely affecting individual Class members.

73. Plaintiffs and members of the Class have all sustained damages during the Class Period as a result of having their personal, confidential information disclosed to unauthorized third parties by Equifax. The conduct alleged herein, the impact of such conduct, and the relief sought are all issues or questions that are common to Plaintiffs and the Class.

74. The questions of law and fact common to the Class include, but are not limited to:

a. whether Equifax engaged in the wrongful conduct alleged herein;

b. whether Equifax owed a duty to Plaintiffs and members of the Class to adequately protect their personal, confidential information and to provide timely and accurate notice of the Equifax Data Breach to Plaintiffs and members of the Class;

c. whether Equifax breached its duty to protect the personal, confidential information of Plaintiffs and members of the Class by failing to provide adequate security;

d. whether Equifax breached its duty to provide timely and accurate notice to Plaintiffs and members of the Class of the Equifax Data Breach;

e. whether Equifax knew or should have known that its systems were vulnerable to attack;

f. whether Equifax's conduct, including its failure to act, resulted in, or was the proximate cause of, the breach of its systems, resulting in the loss of millions of individuals' personal, confidential data;

g. whether Equifax unlawfully failed to inform Plaintiffs and members of the Class that it did not maintain security systems, practices, and protocols adequate to reasonably safeguard their personal, confidential data;

h. whether Equifax's conduct constituted a breach of the FCRA;

i. whether Equifax's conduct constituted unfair methods of competition or was deceptive, unfair, or otherwise unlawful;

j. whether Plaintiffs and members of the Class were injured by Equifax's conduct (or failure to act), and, if so, the appropriate class-wide measure of damages; and

k. whether Plaintiffs and members of the Class are entitled to equitable relief.

75. *Superiority*. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because joinder of all members of the Classes is impracticable.

76. The prosecution of separate actions by individual members of the Class would impose heavy burdens upon the courts and the parties, and would create a risk of inconsistent or varying adjudications of the questions of law and fact common to the Class. A class action would achieve substantial economies of time, effort, and expense, and would assure uniformity of decision as to persons similarly situated without sacrificing procedural fairness. There will be no material difficulty in the management of this action as a class action on behalf of the Class. Although the laws of different states are implicated in this Complaint, these laws are substantially similar to one another and can be grouped together in manageable categories.

77. Because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and because a class action is superior to other available methods for the fair and efficient adjudication of the controversy, class certification is appropriate under Fed. R. Civ. P. 23(a) and (b)(3).

78. Certification of the Class is also appropriate pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and/or (c)(4).

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Negligence

79. Plaintiffs incorporate and reallege, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

80. Equifax owed a duty of care to Plaintiffs and the Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting their personal and financial information in its possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Equifax's security system to ensure that the personal and financial information of Plaintiffs and the Class members was adequately secured and protected.

81. Equifax owed a duty of care to Plaintiffs and the Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

82. Equifax owed a duty of care to Plaintiffs and the Class members to provide security, including security consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of Plaintiffs and the Class members.

83. Equifax owed a duty of care to Plaintiffs and the Class members because they were foreseeable and probable victims of any inadequate security practices. Equifax solicited, gathered, and stored the personal and financial data of Plaintiffs and the Class members to facilitate credit reports and monitoring. Equifax knew or should have known

it inadequately safeguarded such information and that hackers routinely attempt to access this valuable data without authorization. Equifax had prior notice that its systems were inadequate by virtue of earlier breaches, but continued to utilize those inadequate systems to the ultimate detriment of its customers, including Plaintiffs, the Class members, and nearly half of the U.S. population. Equifax knew or should have known that a breach of its systems would cause damages to Plaintiffs and the Class members, and Equifax had a duty to adequately protect such sensitive personal and financial information.

84. Equifax owed a duty of care to timely and accurately disclose to Plaintiffs and the Class members that their personal and financial information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate, and necessary so that, among other things, Plaintiffs and the Class members could take appropriate measures to avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Equifax's misconduct.

85. Equifax knew or should have known of the risks inherent in collecting and storing the personal and financial information of Plaintiffs and the Class members, and of the critical importance of providing adequate security of that information.

86. Equifax's conduct created a foreseeable risk of harm to Plaintiffs and the Class members. Equifax's misconduct included, but was not limited to, its failure to take steps to prevent the Equifax Data Breach from occurring, its failure to stop the breach once it started, its failure to take appropriate action to mitigate the effects of the breach, and its failure to timely inform the public, including Plaintiffs and the Class members, of its occurrence.

87. Equifax breached the duties it owed to Plaintiffs and the Class members by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the personal and financial information of Plaintiffs and the Class members.

88. Equifax breached the duties it owed to Plaintiffs and the Class members by failing to properly implement technical systems or security practices that could have prevented the loss of data at issue.

89. Equifax breached the duties it owed to Plaintiffs and the Class members to timely and accurately disclose that their personal and financial information had been or was reasonably believed to have been stolen or otherwise compromised.

90. But for Equifax's wrongful and negligent breach of the duties owed to Plaintiffs and the Class members, their personal and financial information would not have been stolen or otherwise compromised.

91. The injury and harm suffered by Plaintiffs and the Class members, as set forth above, was the reasonably foreseeable result of Equifax's failure to exercise reasonable care in safeguarding and protecting the personal and financial information of Plaintiffs and the Class members. Equifax knew or should have known that its systems and technologies for processing, securing, and safeguarding the personal and financial information of Plaintiffs and the Class were inadequate and vulnerable to being breached by hackers.

92. Plaintiffs and the Class members suffered injuries and losses described herein as a direct and proximate result of Equifax's conduct resulting in the Equifax Data Breach, including Equifax's lack of adequate reasonable and industry-standard security measures. Had Equifax implemented such adequate and reasonable security measures, Plaintiffs and the Class members would not have suffered the injuries alleged, as the Equifax Data Breach would likely have not occurred.

93. Equifax's conduct also warrants moral blame, as Equifax continued to take possession of Plaintiffs' and the Class members' personal and financial information in connection with its services at a time it knew, but failed to disclose, that it had inadequate systems to reasonably protect such information. Equifax continued to take possession Plaintiffs' and the Class members' personal and financial information after it knew the Equifax Data Breach had occurred and was ongoing, and it failed to provide timely and adequate notice to Plaintiffs and the Class members of that breach as required by law.

94. Holding Equifax accountable will further the policies underlying negligence law and will require Equifax (while also encouraging similar companies that obtain and retain sensitive consumer personal and financial information) to adopt, maintain, and properly implement reasonable, adequate and industry-standard security measures to protect such customer information.

95. As a direct and proximate result of Equifax's negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in the amount to be proven at trial.

SECOND CLAIM FOR RELIEF
Willful Violation of the FCRA

96. Plaintiffs incorporate and reallege each and every allegation set forth in the preceding paragraphs of this Complaint as though fully set forth herein.

97. The FCRA was enacted "to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this [Act]." 15 U.S.C. § 1681(b).

98. Plaintiffs, the Class members, and Defendant Equifax are all "persons" within the meaning of 15 U.S.C. § 1681a(b).

99. Plaintiff and the Class members are "consumers" within the meaning of 15 U.S.C. § 1681a(c).

100. Defendant Equifax is a "person which, for monetary fees . . . regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." As such, Defendant Equifax is a "consumer reporting agency" within the meaning of 15 U.S.C. §1681a(f).

101. As a CRA, Equifax is statutorily required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 604 [15 USCS § 1681b]." 15 U.S.C. § 1681e(a).

102. Under the FCRA, the term "consumer report" means "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for - - (A) credit or insurance to be used primarily for personal, family or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 604 [15 U.S.C. § 1681b]." 15 U.S.C. § 1681a(d)(1)(A)-(C).

103. Because the information Equifax disclosed and communicated to third parties in the Equifax Data Breach included information bearing on Plaintiffs' and the Class members' "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living," and because Equifax had collected that information "in whole or in part for the purpose of serving as a factor in establishing [their] eligibility for - - credit or insurance to be used primarily for personal, family or household

purposes," the disclosures Equifax made in the Equifax Data Breach constitute "credit reports" within the meaning of the FCRA.

104. Pursuant to the FCRA, Equifax "may furnish a consumer report" only under certain statutorily enumerated circumstances, "and no other." 15 U.S.C. § 1681b(a). Those circumstances (which are set forth at 15 U.S.C. § 1681b) do not include furnishing consumer reports to hackers, cyber attackers, or other unauthorized/unidentified third parties.

105. Equifax willfully violated 15 U.S.C. § 1681e(a) by failing to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 604 [15 U.S.C. § 1681b]," and it willfully violated 15 U.S.C. § 1681b by failing to take reasonable measures to protect the sensitive consumer credit information of Plaintiffs and the Class members,[43] and/or by furnishing consumer reports under circumstances other than those specifically authorized by the FCRA.

106. An illustrative, but by no means exhaustive, list of Equifax's willful conduct (which is set forth in detail in the preceding paragraphs) includes the following: (a) Equifax knew about the value placed on the information it exposed in Equifax Data Breach and the corresponding importance of protecting it from unauthorized disclosure; (b) Equifax knew of its legal obligations to protect the information it exposed in the Equifax Data Breach; (c) Equifax knew – by virtue of having been the target of several previous successful hacks/cyber-attacks that resulted in the disclosure of the same type of sensitive information – that is security systems, procedures, and protocols are (and have long been) vulnerable

[43] Indeed, the FTC has made it clear that entities which "fail[] to take reasonable measures to protect sensitive consumer information" violate the FCRA, and that it "will call for imposition of civil penalties against resellers of consumer reports who do not take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the Fair Credit Reporting Act ('FCRA')." https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-brill-which-chairman-leibowitz-and-commissioners-rosch-and-ramirez-join/110125settlementone.pdf

and inadequate to protect the sensitive information with which it has been entrusted; (d) Equifax knew about the vulnerability/inadequacy of its security systems by virtue of having been previously provided with "clear and simple instructions of how to remedy the situation;"[44] and (e) despite the foregoing knowledge Equifax did nothing, thus ensuring it was "relatively easy" for attackers to gain access to its servers and network.[45] Additionally, once the attackers gained access and the Equifax Data Breach commenced, Equifax, with knowledge of the fact that the breach had occurred, waited for over a month to report it to the public, during which time its top executives sold their stock.

107. Ultimately, Equifax's willful conduct provided a means for unauthorized third parties to obtain consumer reports relative to Plaintiffs and the Class members, and Equifax furnished those consumer reports for purposes not authorized by, and in violation of, the FCRA.

108. As a direct and proximate result of Equifax's willful violations of the FCRA, Plaintiff and the Class members are entitled to recover "any actual damages sustained . . . of not less than $100 and not more than $1,000;" to recover "such amount of punitive damages as the court may allow;" and to recover "the costs of the action together with reasonable attorney's fees as determined by the court." 15 U.S.C. § 1681n(a)(1)-(3).

THIRD CLAIM FOR RELIEF
Negligent Violation of the FCRA

109. Plaintiffs incorporate and reallege each and every allegation set forth in the preceding paragraphs of this Complaint as though fully set forth herein.

110. Equifax was negligent in failing to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed" under 15 U.S.C. § 1681b, in failing to take reasonable measures to protect the sensitive consumer credit

[44] https://www.wired.com/story/equifax-breach-no-excuse/
[45] *Id.*

information of Plaintiffs and the Class members, in furnishing consumer reports under circumstances other than those specifically authorized by the FCRA, and in failing to timely notify the public and/or take appropriate remedial action after becoming aware of the breach.

111. Equifax's negligent acts and omissions provided a means for unauthorized third parties to obtain consumer reports relative to Plaintiffs and the Class members, and Equifax furnished those consumer reports for purposes not authorized by, and in violation of, the FCRA.

112. An illustrative, but by no means exhaustive, list of Equifax's negligent conduct (which is set forth in detail in the preceding paragraphs) includes the following: (a) Equifax knew or should have known about the value placed on the information it exposed in Equifax Data Breach and the corresponding importance of protecting it from unauthorized disclosure; (b) Equifax knew or should have known of its legal obligations to protect the information it exposed in the Equifax Data Breach; (c) Equifax knew or should have known – by virtue of having been the target of several previous successful hacks/cyber-attacks that resulted in the disclosure of the same type of sensitive information – that is security systems, processes, and protocols are (and have long been) vulnerable and inadequate to protect the sensitive information with which it has been entrusted; (d) Equifax knew or should have known about the vulnerability/inadequacy of its security systems, processes, and protocols, by virtue of having previously been provided with "clear and simple instructions of how to remedy the situation;"[46] and (e) despite the foregoing knowledge Equifax did nothing, thus ensuring it was "relatively easy" for attackers to gain access to its servers and network.[47] Additionally, once the attackers gained access and the Equifax Data Breach commenced, Equifax, with full knowledge of the fact that the breach

[46] https://www.wired.com/story/equifax-breach-no-excuse/
[47] *Id.*

had occurred, waited for over a month to report it to the public, during which time its top executives sold their stock.

113. As a direct and proximate result of Equifax's negligent violations of the FCRA, Plaintiff and the Class members are entitled to recover "any actual damages sustained," and to recover "the costs of the action together with reasonable attorney's fees as determined by the court." 15 U.S.C. § 1681o(a)(1)-(2).

FOURTH CLAIM FOR RELIEF
Violations of State Consumer Protection Laws

114. Plaintiffs incorporate and reallege each and every allegation set forth in the preceding paragraphs of this Complaint as though fully set forth herein.

115. Equifax engaged in conduct that was intended to result, and that did result, in the sale of goods or services to consumers, including Plaintiffs and the Class members.

116. Equifax is engaged in, and its acts and omissions affect, trade and commerce. Equifax undertook those acts and omissions (which are set forth at length in the preceding paragraphs), in the course of its business of marketing, offering for sale, and selling goods or services throughout the United States, including in this District.

117. By reason of the conduct and omission of material facts described in this Complaint, Equifax violated state consumer protection laws which prohibit entities like Equifax from representing that goods or services have sponsorship, approval, characteristics, uses or benefits that they do not have, from representing that goods or services are of a particular standard, quality, or grade, if they are of another, and from engaging an any conduct that creates a likelihood of confusion or misunderstanding.

118. By reason of the conduct and omission of material facts described in this Complaint, Equifax violated state consumer protection laws that prohibit unfair methods of competition and unfair, deceptive, unconscionable, fraudulent or unlawful trade acts or practices; specifically:

- California Consumer Legal Remedies Act – Cal. Civ. Code § 1750 *et seq*., including Cal. Civ. Code § 1770(a)(5) and (7);[48]
- California Unfair Competition Law – Cal. Bus. & Prof. Code § 17200 *et seq*.;
- Colorado Consumer Protection Act – Colo. Rev. Stat. § 6-1-101 *et seq*., including Colo. Rev. Stat. § 105(1)(b), (e), and (g);
- Florida Deceptive and Unfair Trade Practices Act – Fla. Stat. Ann. § 501.204(1);
- Illinois Consumer Fraud and Deceptive Trade Practices Act – 815 ILCS § 505/2;
- Illinois Deceptive Trade Practices Act – 815 Ill. Stat § 510/2(a)(5), (7) and (12);
- Minnesota Consumer Fraud Act – Minn. Stat. § 325F.69, subd. 1;
- Minnesota Uniform Deceptive Trade Practices Act – Minn. Stat. § 325D.44, subd. 1(5), (7), and (13);
- New Hampshire Consumer Protection Act – N.H. Rev. Stat. § 358-A:2(V) and (VII);
- N.Y Gen. Bus. Law § 349; and
- Wisconsin Deceptive Trade Practices Act – W.S.A. §100.20(1).

119. As a direct and proximate result of Equifax's violation of the foregoing statutes, Plaintiffs and the Class members have suffered damages as set forth above, and as to be proved at trial.

120. Plaintiffs bring this action on behalf of themselves and all others similarly situated for the relief requested and for the public benefit, in order to promote the public interest in the provision of truthful, non-deceptive information, and to protect the public

[48] Plaintiffs do not seek monetary damages at this point in connection with the CLRA claim, but limit their request to injunctive relief. Plaintiffs will seek to amend their Complaint to seek damages in accordance with the CLRA, if Defendant does not correct the harms it has caused after Plaintiffs have provided notice pursuant to California Civil Code §1782.

from Equifax's unfair methods of competition and its unfair, deceptive, fraudulent, unconscionable or otherwise unlawful conduct. Equifax's conduct and omission of material facts, as described in this Complaint, has had widespread impact on the public at large, including causing injury and ascertainable losses of money or property to over 140 million persons across the United States.

FIFTH CLAIM FOR RELIEF
Violations of State Data Breach Statutes

121. Plaintiffs incorporate and reallege each and every allegation set forth in the preceding paragraphs of this Complaint as though fully set forth herein.

122. Legislatures in each of the States listed below have enacted statutes that require any person or entity who conducts business that results in the ownership or licensing of computerized data that includes personal information to protect that information and to disclose any breach of its security system to any resident whose personal information has been acquired by an unauthorized person. Those statutes further require that the disclosure of the breach be made expediently and without unreasonable delay.

123. As noted previously, Equifax learned of the Equifax Data Breach on July 29, 2017, but it concealed information regarding its occurrence for over a month (until September 7, 2017), during which time top Equifax executives executed over $1.8 million in stock options.[49] Had Equifax provided timely and accurate notice of the data breach, Plaintiffs and the Class members would have been able to avoid or mitigate the injuries and damages they have suffered by reason of its occurrence.

124. The Equifax Data Breach constitutes a breach of the Equifax security system within the meaning of the statutes identified below, and the information disclosed in the Equifax Data Breach was covered by these statutes. Accordingly, Equifax's failure to

[49] https://www.cnbc.com/2017/09/07/equifax-cyberattack-three-executives-sold-shares-worth-nearly-2-million-days-after-data-breach.html

provide timely and accurate notice of the Equifax Data Breach constitutes a violation of the following statutes:

- Cal. Civ. Code § 1798.82(a), *et seq.*;
- Colo. Rev. Stat. § 6-1-716(2), *et seq.*;
- Fla. Stat. § 501.171(4), *et seq.*;
- 815 ILCS § 530/10(a), *et seq.*;
- Minn. Stat. Ann. § 325E.61(a), *et seq.*;
- N.H. Rev. Stat. §359-C:20(1)(a), *et seq.*;
- N.Y. Gen. Bus. Law 899-aa, *et seq.*; and
- Wis. Stat. § 134.98(2), *et seq.*

125. As a direct and proximate result of Equifax's violation of the foregoing statutes, Plaintiffs and the Class members have suffered damages as set forth above, and as to be proved at trial.

126. Plaintiffs, on behalf of themselves and all others similarly situated, seek all remedies available under their respective state data breach statutes, including but not limited to damages suffered by Plaintiffs and the Class members as alleged previously; equitable relief, including injunctive relief; and reasonable attorney's fees and costs, as provided by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court:

A. Determine that the claims alleged herein may be maintained as a Class action under Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, and Order that reasonable notice of this action be given to members of the Classes;

B. Appoint Plaintiffs as Class Representatives for the Class and Counsel of Record as Lead Class counsel;

C. Award Plaintiffs and the Class appropriate relief to the maximum extent allowed, and enter a joint and several judgment in favor of Plaintiffs and the Class members, including actual and statutory damages (except that Plaintiffs do not seek damages on their CLRA claim at this time; see footnote 48, above);

D. Award Plaintiffs and the Class equitable, injunctive and declaratory relief as maybe appropriate under applicable state laws. Plaintiffs, on behalf of the Class, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by requiring Equifax to adopt and implement the best security data practices to safeguard customers' financial and personal information, which would include, without limitation, an order and judgment directing Equifax to: (1) encrypt and protect all data; and (2) directing Equifax to provide to Plaintiffs and Class members extended credit monitoring services.

E. Award Plaintiffs and the members of the Class pre- and post- judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of this Complaint;

F. Award Plaintiffs and the members of the Class their costs of suit, including reasonable attorneys' fees, as provided by law; and,

G. Award Plaintiffs and members of the Class such other and further relief as the case may require and the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury, including pursuant to Federal Rule of Civil Procedure 38(b), on all issues where a right to such trial exists.

Respectfully submitted,

Dated: September 29, 2017.

SHULMAN LAW

s/ Harry Shulman
Harry Shulman
44 Montgomery St., Ste. 3830
San Francisco, CA 94104
415-901-0505
harry@shulmanlawfirm.com

Additional counsel, for whom pro hac vice admissions will be sought:

HALUNEN LAW

Melissa W. Weiner, MN #387900
Clayton D. Halunen, MN #219721
Christopher J. Moreland, MN #278142
Charles D. Moore, MN # 396066
80 S. 8th Street, Suite 1650
Minneapolis, MN 55402
Telephone: (612) 605-4098
Facsimile: (612) 605-4099
weiner@halunelaw.com
halunen@halunenlaw.com
moreland@halunenlaw.com
moore@halunenlaw.com

Attorneys for Plaintiffs